UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/733,713 | 12/11/2003 | Clark Debs Jeffries | END920030137US1 | 8632 |

37945 7590 03/29/2007

DUKE W. YEE
YEE AND ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

| EXAMINER | |
|---|---|
| WANG, HARRIS C | |
| ART UNIT | PAPER NUMBER |
| 2139 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 03/29/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/733,713 | JEFFRIES ET AL. | |
| | Examiner | Art Unit | |
| | Harris C. Wang | 2139 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *11 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/11/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-24 are pending

### *Drawings*

2.

The drawings are objected to because In Fig. 5, step 514, Applicant writes:

rs = CHALLENGE + HASH ($g^{XY}$, idpw_digest, rc), when it should read:

rs = CHALLENGE $\oplus$ HASH ($g^{XY}$, idpw_digest, rc), as indicated in Applicant's own specification.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New

Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

***Claim Rejections - 35 USC § 103***

3.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-3, 6-11,14-19 and 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peyravian (6792533) in view of ATIS committee.

Regarding Claim 1,

Peyvarian teaches the computer network, comprising: a client and a server connected by a network connection,

wherein the client has a userid and a password associated with the client *("The user submits his userid (id) and password (pw) to the client" pg. 4)*;

wherein the client requests access to the server by sending a first set of values to the server *("The client generates a random value (rc) and sends id and rc to the server" pg. 4)*;

wherein the server responds to the client by generating a first random value and sending the token to the client; *("The server generates a random value (rs) and sends it to the client" pg. 4). The Examiner interprets the nonce (rs) as the token.*

wherein the client retrieves the first random value from the challenge token and sends the first random value and the userid to the server; *("the client sends id and auth_token to the receiver" pg. 4, the auth_token is comprised of a hash of inputs idpw_digest, rc, and rs, the Examiner interprets rs as both the random value and token")*

wherein the server verifies the received first random value from the client is correct, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server. *("the server verifies the validity of auth_token. If it is valid, the server sends a message to the client giving him permission to access the server" pg. 4)*

Peyvarian does not explicitly teach the server responds to the client by generating a one-time challenge token that depends at least on a first random value and sending the challenge token to the client;

The ATIS Committee defines a message authentication code (MAC) as "A bit string that is a function of both data (either plaintext or ciphertext) and a secret key, and that is attached to the data in order to allow data authentication."

It would have been obvious to one of ordinary skill in the art at the time of the invention to use a MAC as a challenge token, where the examiner interprets the challenge token as data encrypted with a secret key.

The motivation to use a MAC is for "allowing a receiver to verify the integrity of the message" (ATIS definition).

Regarding Claim 2

Peyravian teaches the computer network of claim 1, wherein the first set of values including a first random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one. *("The client generates a random value and sends id and rc to the server" pg. 4).*

Regarding Claim 3,

Peyravian teaches the computer network of claim 1, wherein the client verifies the validity of the one-time authentication token. It is inherent that if a MAC or challenge is sent, the client inherently needs to verify the validity of the token.

Regarding Claim 6,

Peyravian and ATIS committee teach the computer network of claim 1, wherein the server verifies the received first random value from the client is correct by comparing the first random value received from the client with the server's stored value of the first random number. As cited earlier the purpose of a MAC is for "allowing a receiver to verify the integrity of the message" (ATIS definition). The Examiner interprets sending the random value as the data, and the act of comparing the value to see if it is the same as verifying the integrity of the message.

Regarding Claims 7 and 8,

Peyravian and ATIS committee teach the computer network of claim 1, wherein the client changes the password by computing a hash of the userid and a new password to form a new digest *(idpw_digest_new = Hash(id, new_pw), pg. 6, Peyravian),* creating a mask *(auth_token_mask, pg. 7, Peyravian)*, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a

result *(protected_idpw_new = protected_idpw_new XOR auth_token_mask, pg. 7, Peyravian)*

and sending the result, the userid, and the message authentication code to the server; *("The client sends id, auth_token, and protected_idpw_digest_new to the server" pg. 7, Peyravian)*

wherein the server retrieves the new digest by exclusive-oring the mask with the received result *("To retrieve idpw_digest_new, the server generates auth_token_mask...and XORs it with the received protected_idpw_digest_new" pg. 7, Peyravian)*, and wherein the server verifies the received message authentication code,

and wherein if the received message authentication code is verified, the server changes the client password. ("If it is valid, the server sends a message to the client accepting the password change", pg. 7, Peyravian).

It is inherent that if the password is changed, the old password will be replaced with a new password.

Regarding Claims 9-11 and 14-16,

These claims teach the computer program product and method associated with the system claims 1-3 and 14-16. As such they are rejected using the same rationale.

Claim 4, 12 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peyravian in view of ATIS committee as applied to claim 1 above, and further in view of Searchsecurity.com.

Regarding Claim 4,

Peyravian and ATIS committee teach the computer network of claim 1. Peyravian does not explicitly teach wherein the server generates the challenge token by exclusive-oring the first random value with a first hash.

Searchsecurity.com defines a one-time pad, and further teaches "with a one-time pad, the encryption algorithm is simply the XOR operation... it is sometimes combined with another algorithm such as MD5."

It would have been obvious to one of ordinary skill in the art to generate the challenge token by XORing the first random value with a first hash.

The motivation to use a one-time pad is because a well known way of encrypting, the motivation to use a hash as one of the inputs to the pad is to alleviate "concert about how truly random the key is."

Regarding Claims 12 and 20,

These claims teach the computer program product and method associated with the system of Claim 4. As such they are rejected using the same rationale.

Claim 5, 13 and 21 rejected under 35 U.S.C. 103(a) as being unpatentable over Peyravian and ATIS committee in view of Searchsecurity.com as applied to claim 4 above, and further in view of Jablon (6792533).

Regarding Claim 5,

Peyravian, ATIS committee and Searchsecurity.com teach the computer network of claim 4. Searchsecurity.com teach one of the inputs of the one-time pad is a secret key and Peyravian teaches sending the hash of a digest of the clients userid and password *(idpw_digest = Hash(id, pw) pg. 4)*. Peyravian further teaches the client sending a second random value to the server. *("The client generates a random value (rc) and sends id and rc to the server" pg. 4)*;

However the above references do not explicitly teach wherein the first hash is a hash of the following: a primitive root of a large prime number raised to a power, a digest of the client's userid and password, and a second random value.

Jablon teaches that Alice uses a hash function h to compute $V_a$ = h("Alice knows", K, M) (Column 10 lines 34-36). Jablon earlier defined $K = Q_A^{Ra} \bmod p$ (Column 9, lines 47-48). Jablon earlier defines $Q_A = g^{Ra} \bmod p$, g and p are well-known numbers, where g is a primitive root of p (Column 4, lines 13-17). The Examiner interprets K as the primitive root of a large prime number raised to a power. The Examiner interprets "Alice knows" as the random value.

It would have been obvious to one of ordinary skill in the art at the time of the invention for Peyravian modifies the hash to further include the inputs of a primitive root of a large number raised to a power, and a second random value.

The motivation is that the results of the key exchange allow for authentication.

Regarding Claims 13 and 21,

These claims teach the computer program product and method associated with the system of Claim 5. As such they are rejected using the same rationale.

***Conclusion***

4.

A definition of the term "Nonce" is included to show that a nonce can be considered a token.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 8-5:30, Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

Tagbi T. Arani
Primary Examiner
312607